Integrated circuit (IC) card processing system for delivery management of application to IC card, selects application by referring database corresponding to common execution environment when application is to be delivered to IC card
Patent Assignee: NTT DATA TSUSHIN KK

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
JP 2001236232	A	20010831	JP 200048658	A	20000225	200162	B

Priority Applications (Number Kind Date): JP 200048658 A (20000225)

Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
JP 2001236232	A		13	G06F-009/445	

Abstract:
JP 2001236232 A

NOVELTY The data about execution environment of application of various IC cards and data about execution environment of application to deliver is stored in a database (6). The stored data is referred to select application corresponding to common execution environment, when application is to be delivered to IC card.

DETAILED DESCRIPTION INDEPENDENT CLAIMS are also included for the following:

(a) IC card;

(b) IC card processing method;

(c) Disk for storing IC card processing software

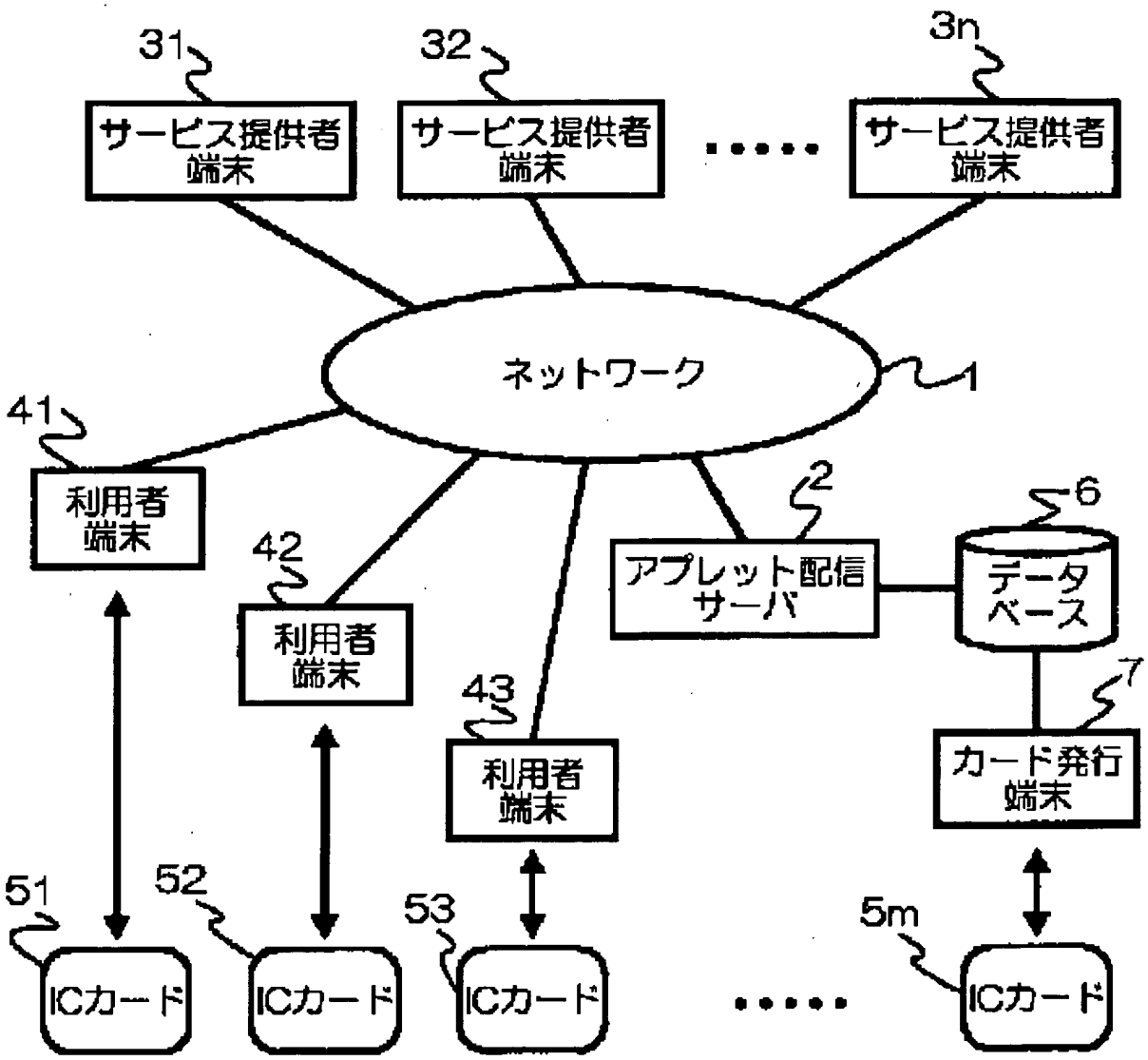
USE For delivery and management of application to IC card, IC chip of portable telephone.

ADVANTAGE Simplifies installation of various applets to IC card.

DESCRIPTION OF DRAWING(S) The figure shows block diagram of IC card processor system.

Database (6)

pp; 13 DwgNo 1/9



410116

Internet based secure transactions using encrypting applets and cgi-scripts independent of browser or server capabilities.

This invention proposes the use of Java applets or ActiveX components executed on a client (browser side) but sent by the server (web server) in order to encrypt the remainder of the communication between the client and the server.

This is especially important and useful as it allows secure transactions under conditions which would normally require special clients and more problematic, special server with appropriate encryption and communication capabilities. Using java applets, or equivalent, to transfer a temporary encryption algorithm to the client the client encrypts accordingly the data using a randomly selected option and an encrypted key sent within the applet code. The data is sent back to the server. It guarantees that only the originating server can decrypt the data.

Currently, it is commonly considered non-acceptable to engage in transactions over the internet without encrypting critical information like credit card numbers. Solutions have been developed to provide secure transactions. All these security systems require that browser as well as server support the encryption schemes and security systems solution. Therefore, all these approaches require significant investments from service providers who must own a server offering the selected type of secure communication or use the service of a company by linking to pages/sites hosted on such compatible servers. For example, when a secure credit card orders is required, a cgi/java or ActiveX script, or an httpd redirection are used to connect to the appropriate page of the secure server provider. Transaction or hosting is thereafter billed to the merchand. :p, This invention propose the use of Java applet, ActiveX or any other code, preferably binary or compiled rather than which is sent by the server and executed on the client during a browser/webserver transaction. The resulting encryption scheme requires only a web server and a browser which are java compatible or which support the appropriate language used instead of Java.

Assuming the use of Java applets, a secure encrypted transaction follows the steps described hereafter:

Server side:

Selection of an encryption scheme, with different encoding and decoding keys. Note that in simplified cases, the encryption key can be the same as the decryption key and both can therefore be public. However the key is always hidden in the java code. Suppose a CGI (Common Gate Interface) script on the server side which compile applets with a random set of keys, selected from a database of acceptable keys. Again this database can be replaced by a code which generates the keys on the fly. The CGI script is called when a user selects the CGI link. It selects randomly a subset of the database, index the keys and encrypts them with an encryption algorithm. In practice this encryption can be extremely simple. A reference number is temporary associated to that particular applet and transaction. The applet is incorporated on the html page returned by the CGI script along with a parameter which designates which key to use. Because the applet is constantly rebuilt, the knowledge of the code used by one version of the applet, obtained by reverse engineering of the binary (byte) code used to extract the key does not help in recovering the keys associated to other transactions. The decoding key is stored on the server with a reference number. Again this can be the same as the encryption key in simple or less critical cases.

Client side

The java code is executed on the client machine. This code recovers the encryption key KK. This may be a recursive process: decrypt the decryption key necessary to decrypt the encryption key by the applet.

At the end of the client side transaction, when data needs to be sent back to the server, the sensitive data is encrypted based on a random key K. K is generated from the encryption key, by modifying it using random a local random generator and a local algorithm run by the applet on the client. The new key K is sent encrypted with the original KK. The data is sent back to the server by the applet calling a CGI script on the server or, even better, by a direct socket connection to the server. This socket connection can always be done if the owner of the server script has administrator privileges on the server. Otherwise, CGI communications may be necessary. Note that other variations including e-mail feedback are also possible but not preferred as it would leave a more permanent track of the transaction.

In the case of a socket connection, the original CGI script, launched when the user selected the secure service, also launched a daemon on the server. This daemon opens a socket, and waits for the answer on the socket from the client. The reference number of the applet/transaction is sent by the client to the server via the socket or as another argument for the new CGI script. The server recovers the decryption key associated to the encryption key KK, decrypt the message, extracts the random key K and decodes the sensitive data.

This whole scheme can run with a very simple java applet and a cgi perl script on the server, along with a java compiler on the server. Note that even if a third party get the encryption key by reverse engineering the java applet byte code, the decoding code remains prohibitive to find, for only ONE possible use: the current transaction using this code.

Applications of the disclosed invention are multiple:
-encryption of credit card order over the internet.
-PayPerView services for web TV or similar pay directly by credit card for a TV program
-Online banking where the customer acts first as a server while the bank is a client when he/she tries to download account information. Thereafter, the roles are reversed when transaction and payment instructions are sent to the bank.
-PIN and smartcard maintenance to initiate, change or revoke the smartcard or PIN number. During request of the service, the customer is the client and the bank is the server. When the maintenance code is sent, the bank becomes the client and the customer is the server.

In summary, this invention is characterized by: 1) Secure and encrypted transactions implemented by sending a code generated from the contacted server to the client, execution on the client, encryption of the data sent back to the server, with a reference data and additional

encryption information useful for the server to decrypt the data. 2) possibility to perform 1) with any type of encryption scheme. 3) Possibility to do this with any code executed on the client side by the server. 4) Usefulness of binary code over scripts 5) Possibility to have socket connections 6) generalization beyond internet protocol to any communication protocol between a requester of a service (client) and provider (server).

Disclosed by International Business Machines Corporation
410116

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－236232
(P2001－236232A)
(43)公開日　平成13年８月31日(2001.8.31)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ　9/445		Ｂ４２Ｄ　15/10	５２１	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｇ０６Ｆ　9/06	５５０Ｂ	５Ｂ０３５
Ｇ０６Ｆ　9/06	５５０	15/00	３１０Ｂ	５Ｂ０５８
15/00	３１０	Ｇ０６Ｋ　17/00	Ｄ	５Ｂ０７６
Ｇ０６Ｋ　17/00		Ｇ０６Ｆ　9/06	４２０Ｌ	５Ｂ０８５

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）　最終頁に続く

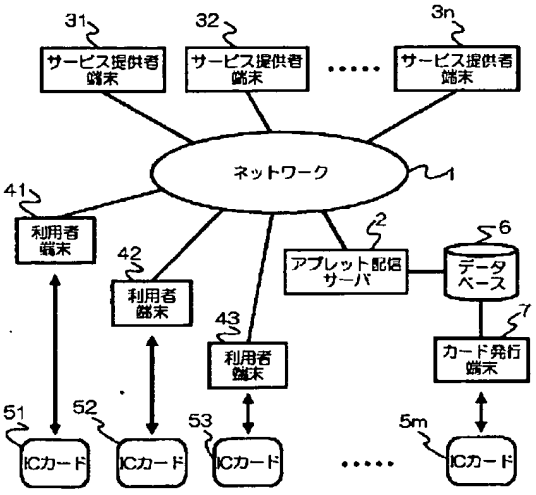
(21)出願番号　特願2000－48658(P2000－48658)
(22)出願日　平成12年２月25日(2000.2.25)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　星川　知之
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　東川　淳紀
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　ＩＣカードシステム、ＩＣカード、ＩＣカード処理方法及び記録媒体

(57)【要約】
【課題】マルチアプリケーション（アプレット）対応のＩＣカードに対して、ＩＣカードに対応したアプレットを容易にダウンロードし、発行することを可能とする。
【解決手段】複数のアプリケーションを搭載可能なＩＣカード５１，５２，５３，…，５ｍを用いてデータ処理を行うＩＣカードシステムにおいて、ＩＣカードへアプリケーションを配信するアプレット配信サーバ２内に、複数のＩＣカードに関するアプリケーションのＯＳの種別等の実行環境に関する情報と、配信するアプリケーションのＯＳの種別等の実行環境に関する情報とを記録管理するデータベース６を管理するためのデータベース管理機能と、ＩＣカード５１，５２，５３，…，５ｍにアプリケーションを配信する際に、データベース６に記憶管理されている情報を参照することで、当該ＩＣカードと共通の実行環境に対応するアプリケーションを選択して配信する自動配信アプレット選択機能を設ける。



1

【特許請求の範囲】

【請求項１】　複数のアプリケーションを搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、

ＩＣカードへアプリケーションを配信する計算機内に、複数のＩＣカードに関するアプリケーションの実行環境に関する情報と、配信するアプリケーションの実行環境に関する情報とを記録管理する記録管理手段と、

ＩＣカードにアプリケーションを配信する際に、記録管理手段に記憶管理されている情報を参照することで、当該ＩＣカードと共通の実行環境に対応するアプリケーションを選択する選択手段とを備えることを特徴とするＩＣカードシステム。

【請求項２】　複数のアプリケーションを搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、

ＩＣカードへアプリケーションを配信する計算機内に、複数のＩＣカードに関するアプリケーションの実行環境に関する情報と、配信するアプリケーションの実行環境に関する情報とを記録管理する記録管理手段と、

ＩＣカードにアプリケーションを配信する際に、記録管理手段に記憶管理されている情報を参照することで、配信対象となるアプリケーションが使用するメモリ容量が、配信先のＩＣカード内の残りのアプリケーション搭載可能メモリ容量よりも小さいか否かを識別するする識別手段とを備えることを特徴とするＩＣカードシステム。

【請求項３】　複数のアプリケーションを搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、

ＩＣカードと、アプリケーションを配信する第１の計算機と、ＩＣカードと第１の計算機との間に介在する第２の計算機とを用いて、ＩＣカードに配信されるアプリケーションに関連する情報を伝送する際に、

第１の計算機において、伝送する情報を暗号化する際に用いる鍵情報を生成する第１の鍵情報生成手段と、

ＩＣカードにおいて、伝送する情報を暗号化する際に用いる鍵情報を生成する第２の鍵情報生成手段とを用い、

第１の計算機において第１の鍵情報生成手段で生成した鍵情報によって伝送データの暗号化処理を行うとともに、第２の計算機において第２の鍵情報生成手段で生成した鍵情報によって伝送データの暗号化処理を行って、第１の計算機と第２の計算機との間で暗号化された情報を送受信することを特徴とするＩＣカードシステム。

【請求項４】　前記第１及び第２の鍵情報生成手段が、各通信セッション毎に新たな鍵情報を生成することを特徴とする請求項３記載のＩＣカードシステム。

【請求項５】　請求項３又は４記載のＩＣカードシステムにおいて、

前記第１の計算機内に、少なくとも配信したアプリケーションに関する情報を各ＩＣカード毎に記憶管理する記憶管理手段を設け、

2

前記第２の計算機が、その記憶管理手段が記憶管理する情報を暗号化処理を行って受信し、該第２の計算機において表示することを特徴とするＩＣカードシステム。

【請求項６】　請求項５記載のＩＣカードシステムにおいて、

ＩＣカードを再発行する際に、前記記憶管理手段内の当該ＩＣカードに関する情報を参照し、再発行前のアプリケーションの配信状況に応じたアプリケーションの配信又は第１の計算機で発行することを特徴とするＩＣカードシステム。

【請求項７】　１つのアプリケーションに関連する情報伝送を複数の通信セッションに分割して行う場合に、

前記第２の計算機において、第１の通信セッションに関連してＩＣカードの認証処理を行うとともに、認証処理の際に当該ＩＣカードに対応して入力された入力情報を暗号化して前記第１の計算機へ送信し、前記第１の計算機において当該ＩＣカードの識別符号に対応させてその入力情報を保存し、

第２の通信セッション以降の通信セッションにおいて、前記第１の計算機において、記憶している入力情報を当該ＩＣカードの識別符号に対応して検索し、前記第２の計算機へ送信し、前記第２の計算機において、受信した入力情報を復号化し、その情報を用いて認証処理を行うことを特徴とする請求項３～６のいずれか１項に記載のＩＣカードシステム。

【請求項８】　請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて用いられることを特徴とするＩＣカード。

【請求項９】　請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて、ＩＣカードへのアプリケーション配信の際にデータ処理方法として用いられるＩＣカード処理方法。

【請求項１０】　請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて用いられるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、マルチアプリケーションを搭載可能なＩＣカードまたは同様の機能を持つＩＣチップを搭載可能な携帯端末や携帯電話システムに対してアプリケーションの配信・管理を行うためのシステムとして、及びそれに利用するＩＣカードとして用いて好適なＩＣカードシステム、ＩＣカード、ＩＣカード処理方法及びそのシステムを実行する際に用いるソフトウェアプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】ＩＣカードには、カード内で所定のプロ

グラムに従って演算処理を行うためのプロセッサと、プログラムやデータを記憶するためのメモリを内蔵したものがある。カード内で行われる演算処理には、暗証番号を確認するための認証処理、データの暗号化および復号化を行うための暗号処理等がある。近年、このようなＩＣカードに複数のアプリケーションプログラムを記録することで、１つのＩＣカードで複数の機能（サービス）を実現するものが提案されてきている。

【０００３】例えば、特開平１０－１２４６２５号公報「ＩＣカードシステム、ＩＣカードおよび記録媒体」には、カード保有者が１枚のＩＣカードに複数のサービスを発行させるための処理方法の一例が記載されている。また、ＩＣカードシステムにおいて、ＩＣカードへのデータの書き込み処理等におけるセキュリティの向上を図った技術の一例が、特開平１０－２８３３２０号公報「セキュリティシステム、機密プログラム管理方法及び記録媒体」に記載されている。この公報に記載されているシステムでは、セキュリティの向上ため、ＩＣカードをアクセスするプログラムを利用者端末（クライアント）に残さない方法を採用している。

【０００４】上記特開平１０－１２４６２５号公報記載の技術では、ＩＣカードで実行される各アプリケーション（アプレット）の暗号処理において用いられる鍵が全てのアプレットで同じものとなっているため、複数のサービス提供者が提供する各アプレットを同時に搭載するＩＣカードシステムでは、相互のサービスの安全性を確保することができない。一方、特開平１０－２８３３２０号公報に記載されている技術では、通信セッションが切れた場合の対策が記述されていない。このように従来の技術では、複数のアプレットが搭載されるＩＣカードの発行（２次発行、サービス申し込み）を安全におこなう相互認証や暗号鍵を利用した手法について、検討すべき課題が残っていた。ここで、ＩＣカードの１次発行とはＩＣカードへのアプレットのロードおよびインストールまでの処理を意味し、２次発行とはＩＣカードへのインストールしたアプレットを利用する際に必要となるデータ（支払い用の電子キャッシュデータ、テレホンカードの度数データ、暗証番号、名前等の個人情報等）の申し込みとサーバへの登録およびＩＣカードへのロードの処理を意味する。

【０００５】また、従来の技術においては、複数のアプレットを２次発行する際のアプレットの代行配信にともなう課金の仕組みに関する規定や、ＩＣカードによる認証とそれに基づく課金、ＩＣカードとセンタで生成した鍵を用いて高速に暗号通信する処理に関する規定についても検討の余地があった。

【０００６】一方、プログラムの配信に関する一般的な関連技術として、特開平１１－２７２４７１号公報「ソフトウェア配信システムとそれに用いるプログラムを記録した記録媒体」に記載されたものや、特開平０５－２７４１２３号公報「ソフトウェアのインスタレーション方法」に記載されたものがある。前者は、配信システムにおけるソフトのバージョンアップ効率法に関するものであり、後者は利用者端末から要求されたソフトがその端末にふさわしくない場合にインルトールを不可とする仕組みに関するものであるが、利用者端末に最適なソフトを選択して配信するものではない。また、両者は、アプリケーションのバージョンや搭載／未搭載を管理する際に用いられる技術である。これに対して、ＩＣカードへのアプレットの配信の際には、複数の発行段階やロック状態があるＩＣカードに関して状態管理を行う処理を規定が必要であったり、複数のアプレットが搭載されるＩＣカードにおいてネットワーク接続されたサーバを用いてその状態を閲覧する処理を規定する必要があったり、あるいは、複数アプレットが搭載されるＩＣカードにおいて、カードの更改を容易にする処理を規定する必要があったりするが、従来の技術ではこれらの点について検討すべき課題が残っていた。

【０００７】

【発明が解決しようとする課題】また、従来の技術では、ＩＣカードに新たにアプレットを追加する場合には、利用者が自分のＩＣカードにあったアプレット（アプリケーションあるいはプログラム）を選択して、配信を希望する必要があった。また、すでにいくつかのアプレットを登録したＩＣカードにおいて、さらに希望するアプレットが容量的に追加可能か否かは実際にアプレットをロードする操作を実行しなければ分からなかった。

【０００８】さらに従来の技術では、安全なアプレットの課金量算出手法ができなかった。これは、暗号処理能力の低いＩＣカードの場合、実用的な速度での認証、秘匿通信ができないことが理由の一つであった。

【０００９】さらに従来の技術では、複数アプレットを搭載するカードを効率的に運用する方法がなかった。複数アプレットの使い勝手がわるかった。複数のアプレット、サービスに対応したカードの場合、各サービスの情報や状態を閲覧する手段がなかった。複数のアプレット、サービスに対応したカードの場合、カード自体の有効期限切れに応じて各サービスの期限を決める必要があった。また、有効期限超過、紛失、故障時のカード内アプレットの復旧、データの復旧に有効な手段がなかった。

【００１０】さらに従来の技術では、異なるサービス提供者が提供するアプレットが複数含まれるＩＣカードの場合、認証処理を行う際には同一の認証や暗号通信の鍵を用いるため、他のサービス提供者による不正が行われる危険性があった。

【００１１】さらに従来の技術では、ネットワークを利用したＩＣカードアクセス処理において、通信セッションが切れるごとにＩＣカードに対して本人認証を複数回行う必要があった。

5

【００１２】本発明は、上記の従来の技術の課題を解決することを目的とするものであって、具体的には、マルチアプリケーション（アプレット）対応のＩＣカードに対して、ＩＣカードに対応したアプレットを容易にダウンロードし、発行を行うことを可能とするＩＣカードシステム、ＩＣカード、及びＩＣカード処理方法を提供することを一つの目的とする。

【００１３】また、本発明は、マルチアプリケーション（アプレット）対応のＩＣカードに対してアプレットをダウンロードするシステムにおいて、またはそれを代行ダウンロードするシステムにおいて、安全に課金を行うことを可能とするＩＣカードシステム、ＩＣカード、及びＩＣカード処理方法を提供することを一つの目的とする。

【００１４】また、本発明は、マルチアプリケーション（アプレット）対応のＩＣカードに対して、ＩＣカードやＩＣカード内アプレットの状態閲覧やカードの更改を容易に行うことを可能とするＩＣカードシステム、ＩＣカード、及びＩＣカード処理方法を提供することを一つの目的とする。

【００１５】また、本発明は、マルチアプリケーション（アプレット）対応のＩＣカードに対して、アプレットをダウンロードし発行するシステムにおいて、安全なサービスの登録（２次発行）を行うこと可能とするＩＣカードシステム、ＩＣカード、及びＩＣカード処理方法を提供することを一つの目的とする。

【００１６】また、本発明は、ネットワークを利用したＩＣカードの本人認証処理において、例えば、アプリケーションの構造上などによって、やむなく通信セッションが切れた場合にも、容易に本人認証を実現すること可能とするＩＣカードシステム、ＩＣカード、及びＩＣカード処理方法を提供することを一つの目的とする。

【００１７】

【課題を解決するための手段】上記課題を解決するため、請求項１記載の発明は、複数のアプリケーション（あるいはアプレット）を搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、ＩＣカードへアプリケーションを配信する計算機内に、複数のＩＣカードに関するアプリケーションの実行環境に関する情報と、配信するアプリケーションの実行環境に関する情報とを記録管理する記録管理手段と、ＩＣカードにアプリケーションを配信する際に、記録管理手段に記憶管理されている情報を参照することで、当該ＩＣカードと共通の実行環境に対応するアプリケーションを選択する選択手段とを備えることを特徴とする。請求項２記載の発明は、複数のアプリケーションを搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、ＩＣカードへアプリケーションを配信する計算機内に、複数のＩＣカードに関するアプリケーションの実行環境に関する情報と、配信するアプリケーションの

6

実行環境に関する情報とを記録管理する記録管理手段と、ＩＣカードにアプリケーションを配信する際に、記録管理手段に記憶管理されている情報を参照することで、配信対象となるアプリケーションが使用するメモリ容量が、配信先のＩＣカード内の残りのアプリケーション搭載可能メモリ容量よりも小さいか否かを識別するする識別手段とを備えることを特徴とする。

【００１８】請求項３記載の発明は、複数のアプリケーションを搭載可能なＩＣカードを用いてデータ処理を行うＩＣカードシステムにおいて、ＩＣカードと、アプリケーションを配信する第１の計算機と、ＩＣカードと第１の計算機との間に介在する第２の計算機とを用いて、ＩＣカードに配信されるアプリケーションに関連する情報を伝送する際に、第１の計算機において、伝送する情報を暗号化する際に用いる鍵情報を生成する第１の鍵情報生成手段と、ＩＣカードにおいて、伝送する情報を暗号化する際に用いる鍵情報を生成する第２の鍵情報生成手段とを用い、第１の計算機において第１の鍵情報生成手段で生成した鍵情報によって伝送データの暗号化処理を行うとともに、第２の計算機において第２の鍵情報生成手段で生成した鍵情報によって伝送データの暗号化処理を行って、第１の計算機と第２の計算機との間で暗号化された情報を送受信することを特徴とする。請求項４記載の発明は、前記第１及び第２の鍵情報生成手段が、各通信セッション毎に新たな鍵情報を生成することを特徴とする。請求項５記載の発明は、請求項３又は４記載のＩＣカードシステムにおいて、前記第１の計算機内に、少なくとも配信したアプリケーションに関する情報を各ＩＣカード毎に記憶管理する記憶管理手段を設け、前記第２の計算機が、その記憶管理手段が記憶管理する情報を暗号化処理を行って受信し、該第２の計算機において表示することを特徴とする。

【００１９】請求項６記載の発明は、請求項５記載のＩＣカードシステムにおいて、ＩＣカードを再発行する際に、前記記憶管理手段内の当該ＩＣカードに関する情報を参照し、再発行前のアプリケーションの配信状況に応じたアプリケーションの配信又は第１の計算機で発行することを特徴とする。請求項７記載の発明は、１つのアプリケーションに関連する情報伝送を複数の通信セッションに分割して行う場合に、前記第２の計算機において、第１の通信セッションに関連してＩＣカードの認証処理を行うとともに、認証処理の際に当該ＩＣカードに対応して入力された入力情報を暗号化して前記第１の計算機へ送信し、前記第１の計算機において当該ＩＣカードの識別符号に対応させてその入力情報を保存し、第２の通信セッション以降の通信セッションにおいて、前記第１の計算機において、記憶している入力情報を当該ＩＣカードの識別符号に対応して検索し、前記第２の計算機へ送信し、前記第２の計算機において、受信した入力情報を復号化し、その情報を用いて認証処理を行うこと

を特徴とする。請求項８記載の発明は、請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて用いられることを特徴とするＩＣカードである。請求項９記載の発明は、請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて、ＩＣカードへのアプリケーション配信の際にデータ処理方法として用いられるＩＣカード処理方法である。請求項１０記載の発明は、請求項１～７のいずれか１項に記載のＩＣカードシステムにおいて用いられるプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００２０】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。図１は、本発明によるＩＣカードシステムのシステム構成を示すブロック図である。図１に示すＩＣカードシステムは、公衆網等のネットワーク１を介して相互に接続されるアプレット配信サーバ２、複数のサービス提供者端末３１，３２，…，３ｎ、および複数の利用者端末４１，４２，４３，…と、利用者端末４１，４２，４３，…に挿入・接続される複数のＩＣカード５１，５２，５３，…，５ｍと、アプレット配信サーバ２において管理されるデータベース６と、データベース６に接続されているカード発行端末７とから構成されている。

【００２１】ＩＣカード５１，５２，５３，…，５ｍは、プロセッサと、ＲＯＭ、ＲＡＭ，ＥＥＰＲＯＭ(Electrically Erasable Programable Read-Only Memory)等のメモリと、外部とのインターフェースとなる回路とから構成されいる。各ＩＣカード５１，５２，５３，…，５ｍには、各ハードウェアを制御するための基本機能を提供するＯＳ（オペレーションシステム）が搭載されていて、そのＯＳの管理の下、複数のアプレット（アプリケーション）をロードおよびインストールして、実行できるようになっている。ＩＣカード用のＯＳとしては、例えば、Java Card（サンマイクロシステムズ社の商標）やWindows for Smart Card（マイクロソフト社の商標）といったものがある。

【００２２】図２を参照して、ＯＳとしてJava Cardを用いる場合のＩＣカード５１，５２，５３，…の構成例について説明する。図２に示すＩＣカードにおいて、複数のアプレットを実行するための基本システムは、マイクロプロセッサ５０１とＯＳ５０２との組み合わせによって実現されている。ＩＣカードの基本機能である標準カードオペレーション、メッセージ管理、ファイル管理、セキュリティ管理、および他の各種基本ユーティリティは、マイクロプロセッサ５０１のハードウェアのみによって、あるいはＯＳ５０２とマイクロプロセッサ５０１との組み合わせによって実現されている。ＯＳ５０２の上では、各アプレットを翻訳して実行するインタプリタとなるJava Card VM（仮想マシン）が実行されている。また、ＩＣカード内のＥＥＰＲＯＭ等のメモリには複数のアプレット５０４ａ，５０４ｂ，５０４ｃが記憶されていて、それらのうちのいずれかが選択されて実行されるようになっている。

【００２３】一方、図１に示すアプレット配信サーバ２は、サービス提供者３１，３２，…によって提供されるサービス（アプレットあるいはアプリケーション）のＩＣカード５１，５２，…への配信を代行するサーバである。アプレット配信サーバ２は、また、データベース６によって、配信する各アプレットを構成するデータと、アプレット配信サーバ２内の各処理（各機能）で利用する複数組のデータとを管理している。ここで、図３を参照して、アプレット配信サーバ２のハードウェアおよびソフトウェアによって実現される各機能について説明する。アプレット配信サーバ２には、サーバ内のマイクロプロセッサ上で稼働するＯＳ２０１と、主にソフトウェアによって実現される機能である自動配信アプレット選択機能２０２、配信可能アプレット識別機能２０３、認証、秘匿配信機能２０４、アプレット状態閲覧機能２０５、およびカード更改、情報修復機能２０６が搭載されている。さらに、アプレット配信サーバ２には、データベース６を管理するためのデータベース管理機能２０７と、サービス提供者端末３１，３２，…、利用者端末４１，４２，…、およびカード発行端末７との間の通信において通信データの送受信の制御を行うインターフェースである通信制御機能２０８とが備えられている。

【００２４】図３に示す自動配信アプレット選択機能２０２は、ＩＣカード５１，５２，…の保持者の要求に応じて、ＩＣカード５１，５２，…に対してそれぞれアプレットを配信する際に、データベース６に登録されている各ＩＣカード５１，５２，…に搭載されているＯＳの種類やバージョンに対応する情報等の各アプレットの実行環境に関する情報に基づいて、適切な（実行可能な）アプレットを自動的に選択して配信する機能である。カード保持者あるいはＩＣカード毎に、Java CardやWindows for Smart Cardといった種類の異なるＩＣカード用のＯＳを搭載したカードが存在する場合、カードの種別（構成）やＯＳによって実行できるアプレット（Applet）の種類が異なるため、自動配信アプレット選択機能２０２では、利用者がアプレットのロードを希望したときに、これを自動的に判別してロードする。

【００２５】一方、配信可能アプレット識別機能２０３は、各アプレットの配信に先立って、各ＩＣカード５１，５２，…内でアプレットを記憶するためのメモリの残り（空き）記憶容量と、データベース６に登録されている各アプレットのインストール時，実行時に使用される記憶容量とを比較して、要求されたアプレットを配信可能かどうかを識別する機能である。ＩＣカードのメモリ容量は限られているため、限られた量のアプレットしか一度にロードできないが、実際にアプレットをロードする前にこのような識別を行うことで、不要なアプレッ

トデータが利用者端末４１，４２，…やＩＣカード５１，５２，…まで転送されるのを防止したり、転送できないことを報知するまでの時間を短くすることが可能となる。また、例えば、利用者端末４１，４２，…において、アプレットのロード要求に対して、そのＩＣカードにロードできる容量のアプレット、できないアプレット、既にロード済みのアプレットを反転・強調、薄色や色の違いによって利用者が識別しやすい形態で、各利用者端末４１，４２，…の表示ディスプレイ等で表示することができる。

【００２６】メモリ容量を確認する際には、アプレットのロードを要求したＩＣカードに対して、残り使用可能メモリ量の出力を要求するコマンドを送り、メモリ量を得る。そして、そのＩＣカードにロードすることを要求されたアプレットの使用メモリ量と比較し、アプレットの使用メモリ量が残り使用可能メモリよりも小さい場合はロード可能、それ以外の場合はロード不可能であるとして、識別結果に対応した表示を行うようにする。または、例えば、カード配信前にあらかじめコマンドを使ってＩＣカード５１，５２，…の使用可能メモリ量を測定し、データベース６に登録しておき、各アプレットの使用メモリ量については、測定用のカードにロードして、その前後にコマンドを使ってカードの使用可能メモリ量を測定して、その差分をアプレットの使用メモリ量としてデータベース６に登録しておく。そして、アプレット配信サーバ２にアクセスがあった時に登録されたカードとアプレットのメモリ量を比較する。

【００２７】アプレット配信サーバ２では、ＩＣカード毎に、搭載されているＯＳ等の種類について、カードＩＤを用いてデータベース６内でカード個別に管理する。また、アプレット配信サーバ２では、サービス提供者の要求に応じて、またはアプレット配信サーバ２に接続されたサービス提供者の登録端末２１，２２，…からの指示に基づいて、データベース６内に配信を代行するアプレットをあらかじめ複数登録しておく。アプレットの配信を求めようとするＩＣカード保持者が、利用者端末４１，４２，…にＩＣカードを挿入し、利用者端末４１，４２，…をアプレット配信サーバ２に接続する操作を行ったときには、アプレット配信サーバ２は、利用者端末４１，４２，…において表示する情報として、配信可能なサービスあるいはアプレットのメニューを提供する。カード保持者が、利用者端末４１，４２，…においてメニューからサービスあるいはサービスに必要な機能を持ったアプレットを選択すると、アプレット配信サーバ２は、ＩＣカードに対してアプレットのロードおよびインストールを行うための処理を行う。このとき、アプレット配信サーバ２の自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３は、カード保持者がサービスを要求したときに、データベース６を参照して対象のＩＣカードが搭載するＯＳの種別を読み出し、対応する適切なアプレットを選択するとともに、選択したアプレットのインストールに使用されるメモリ容量がＩＣカードの残りメモリ容量よりも小さいときにのみ、ＩＣカードにそのアプレットをダウンロードするような処理を実行する。

【００２８】ここで、図４を参照して、自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３による処理の具体例について説明する。まず、この説明において用いる図１のデータベース６で管理する各データの構成例を図６～図８を参照して説明する。

【００２９】図６は、複数のサービス提供者の要求に応じて登録されている複数のアプレットに対応するＯＳ情報、ＩＣカードの種別（ハードウェア仕様）情報、メモリ使用量情報等のアプレットの実行環境に関する情報、課金情報、アプレットの配信回数、アプレットの有効期間に関する情報等のデータからなる管理テーブルの一例を示している。この場合、サービス提供者Ｓ１によって、サービス名称ＳＶ１およびＳＶ２の２種類サービスが登録されている。サービス提供者Ｓ２からは、サービス名称ＳＶ３およびＳＶ４の２種類サービスが登録されている。サービス名称ＳＶ１のサービスには、ＯＳ１に対応するアプレットＩＤ（ＡＰＩＤ１）のアプレットと、ＯＳ１と異なるＯＳ２に対応するアプレットＩＤ（ＡＰＩＤ２）のアプレットとが対応し、サービス名称ＳＶ２のサービスには、ＯＳ１に対応するアプレットＩＤ（ＡＰＩＤ３）のアプレットと、ＯＳ２に対応するアプレットＩＤ（ＡＰＩＤ４）のアプレットとが対応している。また、アプレットＡＰＩＤ１、２，３，および４の各アプレットに対しては、それに対応する情報として、対応ＩＣ種別がそれぞれＣ１，Ｃ１、Ｃ２，およびＣ３、メモリ使用量がＭ１，Ｍ２，Ｍ３，およびＭ４、アプレットの各ダウンロードにおける単位課金情報（サービス提供者およびＩＣカード利用者の双方または一方への課金情報）がそれぞれＵＣ１，ＵＣ１，ＵＣ２およびＵＣ２、各アプレットのロード回数（配信回数）がそれぞれＮ１，Ｎ２，Ｎ３，およびＮ４、そして、有効期間がそれぞれＲ１，Ｒ２，Ｒ３，およびＲ４として登録されている。一方、サービス名称ＳＶ３のサービスには、ＯＳ１に対応するアプレットＩＤ（ＡＰＩＤ５）のアプレットのみが対応し、サービス名称ＳＶ４のサービスには、ＯＳ１に対応するアプレットＩＤ（ＡＰＩＤ６）のアプレットのみが対応している。また、アプレットＡＰＩＤ５，６の各アプレットには、対応ＩＣ種別としてそれぞれＣ１およびＣ４，Ｃ４、メモリ使用量としてＭ５，Ｍ６、アプレットの単位課金情報としてそれぞれＵＣ３，ＵＣ４、各アプレットのロード回数としてそれぞれＮ５，Ｎ６、そして、有効期間としてそれぞれＲ５，Ｒ６が対応づけられている。

【００３０】図７は、ＩＣカード個別に決定されているカードＩＤ（カード識別情報）に対応するカード種別情

報と対応ＯＳ情報の各データからなる管理テーブルの一例を示している。この図に示す例においては、カードＩＤ、ＣＤＩＤ１，ＣＤＩＤ２，ＣＤＩＤ３に対応して、カード種別Ｃ１，Ｃ４、Ｃ１と、ＯＳ種別ＯＳ１，ＯＳ１，ＯＳ２とが対応するように登録されている。図８は、各ユーザ（カード保持者）がダウンロードしたアプレットの履歴に関する情報を記録するテーブルを示している。この場合、各ユーザすなわちユーザＩＤ毎に、カードＩＤと、アプレットＩＤと、ＩＣカードの残り使用可能メモリ量と、アプレットの有効期限の情報と、カードの有効期限とが対応して逐次変化が生じる毎に記録されるようになっている。ユーザＩＤ、ＵＩＤ１に対しては、２つのカードＩＤ（ＣＤＩＤ１とＤＣＩＤ２）が登録されていて、一方、ＣＤＩＤ１のカードＩＤに対してはそのカードにインストール済みの２つのアプレットのＩＤ（ＡＰＩＤ１とＡＰＩＤ５）と、そのカードの残り使用可能メモリ量ＵＭ１と、各アプレットの有効期限Ｐ１，Ｐ２と、カードの有効期限Ｑ１が登録されていて、他方、ＣＤＩＤ２のカードＩＤに対してはそのカードにインストール済みの１つのアプレットのＩＤ（ＡＰＩＤ６）と、そのカードの残り使用可能メモリ量ＵＭ２と、そのアプレットの有効期限Ｐ３と、カードの有効期限Ｑ２が登録されている。ユーザＩＤ、ＵＩＤ２に対しては、１つのカードＩＤ、ＣＤＩＤ３と、１つのアプレットＡＰＩＤ２と、残り使用可能メモリ量ＵＭ３と、そのアプレットの有効期限Ｐ４と、カードの有効期限Ｑ３が記録されている。

【００３１】では、図４を参照して、自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３による処理の一具体例について説明する。なお、データベース６内には予め図６～図８に示すような各テーブルと、配信すべき各アプレットのデータが登録されているものとする。いま、利用者端末４１，４２，…のいずれか（ここでは利用者端末４１とする）にＩＣカード５１，５２，…のいずれか（ここではＩＣカード５１とする）を挿入・接続したとする（４０１）。利用者端末４１では、カード保持者からの認証情報をもとに認証処理を行った後、カードＩＤ（ここではＣＤＩＤ１とする）をアプレット配信サーバ２に送信する（４０２）。アプレット配信サーバ２では、図７に示すテーブルを参照してカードＩＤ（ＣＤＩＤ１）に対応するＯＳ種別（ＯＳ１）とカード種別（Ｃ１）を読み取るとともに、図８に示すテーブルを参照して、カードの有効期限をチェックして、期限切れであれば期限切れであると表示する（４０３）。次に、アプレット配信サーバ２は、図６に示すテーブルを参照して、読み取ったＯＳ種別（ＯＳ１）とカード種別（Ｃ１）で提供可能なアプレットＩＤを検索し、アプレットＩＤ（ＡＰＩＤ１，ＡＰＩＤ５）あるいはサービス名称（ＳＶ１，ＳＶ３）の一覧データを利用者端末４１に送信する（４０４）。利用者端末４１では、送られてきた情報に基づいてアプレットＩＤあるいはサービス名称の一覧を表示する（４０５）。

【００３２】ここで、利用者端末４１で、１つ（または複数）のアプレットＩＤあるいはサービスが選択されると、選択結果を示す情報がアプレット配信サーバ２へ送信される（４０６）。次に、アプレット配信サーバ２は、ＩＣカード５１の残り使用可能なメモリ容量の出力要求を行い（４０７）、利用者端末４１を経由して、ＩＣカード５１に対して、残り使用可能なメモリ容量の出力コマンドを発行する（４０８）。ＩＣカード５１が残り使用可能なメモリ容量の値を返してきたら（４０９）、利用者端末４１は、それをアプレット配信サーバ２へ転送する（４１０）。アプレット配信サーバ２では、ＩＣカード５１の残り使用可能なメモリ容量を一旦、図８のデータテーブルに記憶した後、選択されたアプレットＩＤに対応する使用メモリ容量を図７に示すテーブルを参照して求め、それらの大小を比較する（４１１）。ここで、アプレットの使用メモリ容量の方が大きい場合には、利用者端末４１でアプレットのロードが不可である旨の表示を行い（４１２）、アプレットの使用メモリ容量が残り使用可能なメモリ容量以下である場合には、アプレットの有効期限（Ｐ１，Ｐ２，…）を、現在の日付に有効期間（Ｒ１，Ｒ２，…）を加えたものに更新するとともに（４１３）、アプレットをロードする旨の表示を行い（４１４）、そして、アプレットを転送する（４１５）。利用者端末４１では、アプレットを受信すると、そのアプレットをＩＣカード５１に書き込む処理を行う（４１６）。さらに、アプレット配信サーバ２で、アプレットがＩＣカードにロードされたことをデータベース６に登録する（４１７）。

【００３３】次に、図５を参照して図４の変形例について説明する。図５に示す処理例では、利用者端末（例えば利用者端末４１）で選択対象のアプレット（サービス）を表示する際に、事前に、当該ＩＤカードに関して、ＯＳ種別、カード種別、残りメモリ量に関して予め確認を行い、インストールが可能であり、かつ、まだインストールされていないアプレット（サービス）に関する情報を選択して表示するようにしている。図５に示す処理例では、まず、例えば、ＩＣカード５１を利用者端末４１へ挿入、接続し（６０１）、カードＩＤをアプレット配信サーバ２へ送信する（６０２）。アプレット配信サーバ２では、データベース６内のカードＩＤ毎およびユーザＩＤ毎の各データテーブルを参照して、当該カードに対応するＯＳ種別，カード種別，残りメモリ容量を読み取るとともに、図８に示すテーブルを参照して、カードの有効期限をチェックして、期限切れであれば期限切れであると表示する（６０３）。アプレット配信サーバ２では、図６に示すデータテーブル内で各アプレットに対するデータを順次検索し（６０５）、当該アプレットＩＤが当該ＩＣカード５１にすでにロード済みであ

るかどうか（６０６）、当該ＩＣカード５１のＯＳ種別やＩＣカード種別が当該アプレットＩＤの情報と一致するかどうか（６０７）、当該ＩＣカード５１の残りメモリ容量が、当該アプレットＩＤの使用メモリ容量に対して充分かどうか（６０８）をそれぞれ確認し、すべての条件を満足するアプレットＩＤを対象アプレットＩＤとして一時記憶する（６０９）。以上の確認をデータベース６に登録されているすべてのアプレットＩＤして行い、データベース６内の検索が終了したときに、一時記憶された対象となるアプレットＩＤに対応するサービスの情報を利用者端末４１へ送信する（６１０）。

【００３４】利用者端末４１では、当該ＩＣカード５１に対して提供可能なサービスの情報を一覧表示する（６１１）。次に、カード保持者に選択されたサービスの情報が、アプレット配信サーバ２へ送信される（６１２）。次に、アプレットの有効期限（Ｐ１，Ｐ２，…）を、現在の日付に有効期間（Ｒ１，Ｒ２，…）を加えたものに更新するとともに（６１３）、アプレット配信サーバ２は選択されたアプレットのデータを利用者端末４１へ送信し（６１４）、利用者端末４１でＩＣカード５１への書き込みが行われる（６１４）。さらに、アプレット配信サーバ２で、アプレットがＩＣカードにロードされたことをデータベース６に登録する（６１６）。

【００３５】上記のように、自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３を設けることによって、事前にサービス提供者がアプレット配信サーバ２にアプレットとその実行環境に関する情報を登録しておけば、カード保持者からの要求に応じてアプレット配信サーバ２からＩＣカードにアップレットのロードおよびインストールを適切かつ自動的に行うことが可能となる。なお、上記の構成は、ＩＣカードにアップレットのロードおよびインストールを行うための構成であって、各サービスの利用の申し込みはサービス提供者のサーバに接続して、個別に申し込みを行うようにすることができる。また、アプレット配信サーバ２内に、要求に応じてアプレットの削除を行う構成を設けるようにすることもできる。

【００３６】さらに、アプレット配信サーバ２内に、ＩＣカードへのアプレットのロードおよびインストール処理に伴い、アプレット個別またはユーザ個別に配信したアプレットの種類と数によって課金量を算出する機能を設けるようにしてもよい。具体的にはアプレットＩＤ、ユーザＩＤを元に、配信されたアプレットの回数をカウントし、アプレットの配信手数料単価（単位課金情報）を回数に掛け合わせ、サービス提供者、ユーザ毎の請求書を作成する。このとき、カードＩＤとアプレットＩＤを元に、ロード・インストール（一次発行）の経過、サービスの申し込み（二次発行）の経過、有効期限等の状態をデータベース６内で管理するようにして、実際にロードなどの処理が行われたときにデータベース６内の各データを更新するようにする。

【００３７】次に、図３に示す認証、秘匿配信機能２０４について詳細に説明する。認証、秘匿配信機能２０４は、アプレット配信サーバ２から各ＩＣカード５１，５２，…へアプレットを配信する際に行う認証処理と、他のデータ転送を暗号化して行う秘匿配信（通信）を実現するための機能である。認証、秘匿配信機能２０４では、ＩＣカード５１，５２，…内と利用者端末４１，４２，…およびアプレット配信サーバ２のそれぞれの間で相互認証を行い、ＩＣカード５１，５２，…とアプレット配信サーバ２の間の通信の暗号化を、利用者端末４１，４２，…とアプレット配信サーバ２間の暗号化通信で補う機能を提供する。具体的には、ＩＣカード５１，５２，…内、利用者端末４１，４２，…、アプレット配信サーバ２の各々の相互認証鍵を用いて、ＩＣカード５１，５２，…と利用者端末４１，４２，…、利用者端末４１，４２，とアプレット配信サーバ２との間で相互認証を行う。その後、ＩＣカード５１，５２，…とアプレット配信サーバ２の乱数を用いて当該通信セッション中で有効となるセッション鍵を生成する。ＩＣカード５１，５２，…は生成した鍵を利用者端末４１，４２，…に送り、その通信におけるアプレット配信サーバ２とＩＣカード５１，５２，…の秘匿通信を、アプレット配信サーバ２と利用者端末間４１，４２，…との間で行う。

【００３８】図９を参照して、認証、秘匿配信機能２０４を実行する際のシステム内の各処理の一例について説明する。認証、秘匿配信機能２０４では、まず、利用者端末４１，４２，…（利用者端末４１とする）において、接続されたＩＣカード５１，５２，…（ＩＣカード５１とする）に対応する認証情報を入力する（８０１）。次に、利用者端末４１は、ＩＣカード５１に入力された認証情報を出力する（８０２）。ＩＣカード５１では入力された認証情報と、予め登録されている認証情報とを比較して認証処理を行い（８０３）、認証の結果をカードＩＤ等のＩＣカード５１の識別情報とともに利用者端末４１へ出力する（８０４）。正常に処理された場合、利用者端末４１は、カードＩＤ等の情報と認証情報とをアプレット配信サーバ２へ送信し（８０５）、アプレット配信サーバ２において、データベース６に登録されている情報と比較することで認証処理を行う（８０６）。アプレット配信サーバ２は、認証処理の結果を利用者端末４１へ送信する（８０７）。ここで、ＩＣカード５１内と利用者端末４１およびアプレット配信サーバ２のそれぞれの間の相互認証処理が完了する。

【００３９】３者間の相互認証が終了した段階で、秘匿通信の１セッションが開始される（８０８）。まず、利用者端末４１が、ＩＣカード５１に乱数の発生を指示し（８０９）、ＩＣカード５１内で乱数が発生される（８１０）。また、アプレット配信サーバ２でも乱数を発生する（８１１）。ここで、ＩＣカード５１とアプレット

配信サーバ２との間で相互に発生した乱数情報を交換する（８１２）。乱数情報をアプレット配信サーバ２から受信したＩＣカード５１内では、受信した乱数とＩＣカード５１内で発生した乱数でセッション鍵を生成する（８１３）。アプレット配信サーバ２では、発生した乱数情報と、ＩＣカード５１から受信した乱数とでセッション鍵を生成する（８１４）。ここで生成される各セッション鍵は、例えば、アプレットの配信時には、１つ以下のアプレットの配信中でのみ有効となるものであって、２以上のアプレットの配信は２以上のセッションに分割して通信を行うようにすることで、異なるアプレットの配信時に同一のセッション鍵が用いられないようにする。また、１つのアプレットを配信する際に複数のセッションにまたがってすなわち中断を伴いながら通信が行われる場合には、複数のセッション鍵が必要となる。また、アプレットの配信以外のデータ通信においては、そのセッション内で通信されるデータに関連するアプレットに対応するようにアプレット対応のデータを反映するようにしてセッション鍵が生成されるようにしておく。次に、ＩＣカード５１は、生成したセッション鍵を利用者端末４１へ送信する（８１５）。

【００４０】これ以降、利用者端末４１では、ＩＣカード５１から受信したセッション鍵を利用して暗号化処理を行ってアプレット配信サーバ２との間でデータ送受信を行い（８１６）、アプレット配信サーバ２では、自サーバ内で生成したセッション鍵を利用して暗号化処理を行って利用者端末４１との間でデータ送受信を行う（８１７）。すなわち、利用者端末４１とＩＣカード５１との間では、必要に応じて非暗号化データによってデータの送受信を行い（８１８）、利用者端末４１とアプレット配信サーバ２との間では、セッション鍵を用いた暗号化データによるデータの送受信が行われる（８１９）。そして、通信セッションが終了すると（８２０）、利用者端末４１およびアプレット配信サーバ２では、セッション鍵が破棄される（８２１，８２２）。

【００４１】再度、利用者端末４１を介して、ＩＣカード５１とアプレット配信サーバ２との間でデータの送受信を行う場合には、認証情報の入力処理（８０１）は繰り返さずに、通信セッションの開始点（８０８）以降の処理を繰り返して実行し、新たなセッション鍵を生成した後、セッション単位の通信が行われる（８２３）。

【００４２】なお、さらに複数の通信セッションに分かれたサービスを提供する場合、利用者端末４１，４２，…にＰＩＮ（personal indentification number）入力や生態情報入力等が行われたときに、その際の識別情報を暗号化して、アプレット配信サーバ２に送信するようにしてもよい。この場合、一つのサービスはカードＩＤをキーとして、テンポラリファイルに上記識別情報を復号化して保存する。次に本人認証が必要となる通信セッション時に保存しておいた上記識別情報をカードＩＤで検索し、暗号化して利用者端末４１，４２，…に送信し、ＩＣカード５１，５２，…に対して本人認証を実行する。テンポラリファイルはサービス停止または一定時間経過後に自動的に消去するという構成を用いることがとができる。

【００４３】また、アプレット配信サーバ２によって、ロード、インストールするアプレット内に相互認証または暗号化またはその両方に必要な鍵を設定しておくようにしてもよい。サービスの申し込みをする際には、サービス提供者のサーバに接続し、設定しておいた鍵とＩＣカード内のアプレットに含まれる鍵を用いて相互認証または暗号化またはその両方を行い、安全に個人情報を利用者端末、サーバ間でやり取りし、サービスの申し込みを終了する。なお、上記各構成においては、ＰＩＮ入力以外にも指紋などの生体情報を利用した本人認証を利用することができる。

【００４４】次に、図３に示すアプレット状態閲覧機能２０５は、利用者端末４１，４２，…あるいはカード発行端末７において、アプレットの状態（ロード・インストール済み、サービス申し込み済み、有効期限切れ、ロック状態等）を確認可能とするための機能である。ここで、確認する各情報はアプレット配信サーバ２のデータベース６から読み出すことになるが、その際、認証、秘匿配信機能２０４によって提供される秘匿通信配信（機能）機能を利用することで、安全に、ＩＣカード内のアプレットの状態を利用者端末等で表示・管理することが可能となる。具体的には、上記方法でカード内アプレットの状態を管理し、データベース６に接続されたカード発行端末７やネットワーク１によって接続された利用者端末４１，４２，…にカードを挿入、もしくはカードＩＤを入力することで、各ＩＣカード内のアプレットの状態を表示する。

【００４５】また、図３に示すカード更改、情報修復機能２０６は、ＩＣカードの有効期限超過、ＩＣカードの紛失、盗難、故障などにより、新規カードに更改しなければならないときに、以前のＩＣカードと同様のサービスを受けられる状態にＩＣカードを発行する機能である。具体的には、上記方法でＩＣカード内アプレットの状態を管理し、更改する新規カード発行後、旧カードに登録されていたアプレットのロード・インストールを行う。サービスの申し込みについては、発行時にサービス提供者のサーバに接続して旧登録情報を用いて行うか、利用者が新規カードを用いてサービス提供者のサーバに接続した場合に旧登録情報を用いて行う。なお、有効期限切れによるカードの更改時は新規カードの有効期限を旧カードの有効期限＋規定の有効期間とする。故障や紛失によるカードの更改時は新規カードの有効期限を旧カードの有効期限と同等にする。

【００４６】以上説明したように、上記実施の形態によれば、ネットワークを利用したＩＣカードの発行やブロ

グラムの配信を行う際の利便性を向上でき、利用者が容易に配信を希望して機能を追加できる。また、機能追加のための時間短縮を図ったり、カード種別にとらわれない汎用的なシステムが容易に実現できる。希望するアプレットが登録可能か否かを容易に判断でき、場合によっては同類の機能を実現する別のアプレットを選択する選択肢があることを容易に識別できる。具体的には、配信代行システムとして、代行配信サービス提供者（アプレット配信サーバ２）にアプレットを登録すると、即座に新規ユーザに登録する機会を提供することができる。配信に必要な設備・費用を低減できる。自動配信アプレット選択機能により、カード保持者である利用者が自分の持つＩＣカードやＯＳの種類、バージョンを気にしないで、アプレットの登録、サービスの申し込みを行える。配信可能アプレット識別機能によりカード保持者である利用者がロードの可能なアプレットとそれ以外を容易に識別できる。

【００４７】さらに、アプレットの配信、課金システムの安全性を向上することができ、暗号処理能力の低いＩＣカードでもセンタと認証、秘匿通信を高速に処理できる。具体的には、カード保持者である利用者が、能力の低い安価なＩＣカードでセキュリティの高い通信が実現できる。不正なセンタからのアプレットの配信を防止できる。アプレット配信（代行）者が、容易に手数料の算出ができ、手数料の請求が行える。不正なＩＣカードへのアプレットの配信を防止できる。

【００４８】さらに、アプレットの状態が変化したり、カードの更改などの運用を効率的に行い、利便性を高める事ができる。カード内のアプレットや対応するサービスの状態をネットワーク端末（携帯電話やセットトップボックス、ネットワークに接続されたＰＣなど）で容易に確認できる。カードの有効期限超過や紛失、故障時に短時間でカードの更改を行える。具体的には、カード保持者である利用者が、複数のアプレットが載るＩＣカードにおいても、現在カードに入っているアプレットの種類、と各アプレットの状態を確認できる。カードの有効期限超過や故障の場合も、容易に複数のアプレットやサービスを引き続き利用できる。アプレットの配信管理（代行）者が、利用者の要望に応じて、容易にカード内のアプレットの種類と各アプレットの状態を通知できる。アプレット提供者であるサービス提供者が、カードの有効期限や故障にかかわらず、アプレットやサービスの有効期限を設定できる。

【００４９】さらに複数のサービス提供者のアプレットが混在するＩＣカードシステムにおいて、サービス提供者が個別に鍵管理を行うことを容易に実現しており、他のサービス提供者による不正が防止できる。具体的には、カード保持者である利用者が、サービス申し込みに入力する氏名、住所、電話番号などの個人情報を安全にサービス提供者に送信できる。サービス提供者が鍵はアプレット個別に設定できるため、他のサービス提供者によって自社のアプレットを勝手に用いられる事がなく、安全にアプレットを利用できる。

【００５０】さらに、１つのサービス内で通信セッションが切れたり、通信障害で通信セクションが切れる場合にもＰＩＮ入力などの本人認証を１回で済ますことができ、操作を容易にすることがきる。具体的には、複数の通信セッションに分かれたサービスを利用する場合も、何度もＰＩＮや生態情報の入力を行わなくて良く、利便性が向上する。

【００５１】なお、本発明によるシステムは、上記の実施の形態に限定されるものではなく、各機能の分散、統合、省略等、適宜変更可能である。また、本発明の適用は、ＩＣカードに限定されることなく、例えば、それに類似した機能を有するＩＣチップを搭載可能な携帯端末、携帯電話システム等に適用可能である。また、本発明によるシステムにおける各処理方法、およびシステム全体としての処理方法は、システムの一部あるいは全体にわたって配置されているマイクロプロセッサ等の電子計算機において実行されるプログラムは、電子計算機読み取り可能な記録媒体に記録して頒布することが可能である。

【００５２】

【発明の効果】以上説明したように、本発明によれば、特に、複数のアプレットを選択、搭載可能なＩＣカードを用いるシステムにおいて、従来のシステムに比べて利便性の高いＩＣカードシステム、ＩＣカード、ＩＣカード処理方法及び記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明によるＩＣカードシステムの実施形態の構成を示すブロック図

【図２】図１に示す各ＩＣカード５１，５２，…を構成するアーキテクチャの一例を示すブロック図

【図３】図１のアプレット配信サーバ２の構成を示すブロック図

【図４】図１のアプレット配信サーバ２によって提供される自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３の処理内容の一例を示すタイミング図

【図５】図４と同じ自動配信アプレット選択機能２０２および配信可能アプレット識別機能２０３による処理内容の他の例を示すタイミング図

【図６】図１のデータベース６によって管理されるデータテーブルの一例を示す図

【図７】図１のデータベース６によって管理されるデータテーブルの一例を示す図

【図８】図１のデータベース６によって管理されるデータテーブルの一例を示す図

【図９】図１のアプレット配信サーバ２によって提供される認証、秘匿配信機能２０４の処理内容の一例を示す

19

タイミング図

【符号の説明】

1　ネットワーク

2　アプレット配信サーバ

３１，３２，３ｎ　サービス提供者端末

４１，４２，４３　利用者端末

５１，５２，５３，５ｍ　ＩＣカード

6　データベース

7　カード発行端末

20

＊２０１　ＯＳ

２０２　自動配信アプレット選択機能

２０３　配信可能アプレット識別機能

２０４　認証、秘匿配信機能

２０５　アプレット状態閲覧機能

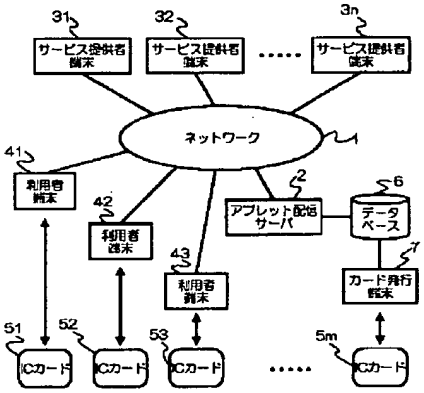
２０６　カード更改、情報修復機能

２０７　データベース管理機能

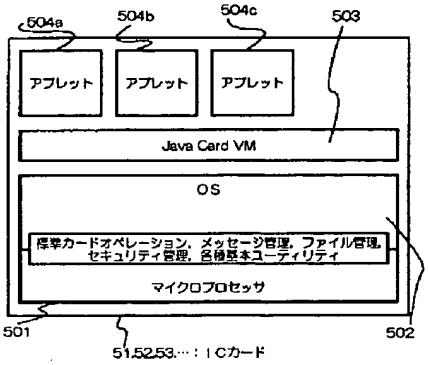
２０８　通信制御機能

＊

【図１】



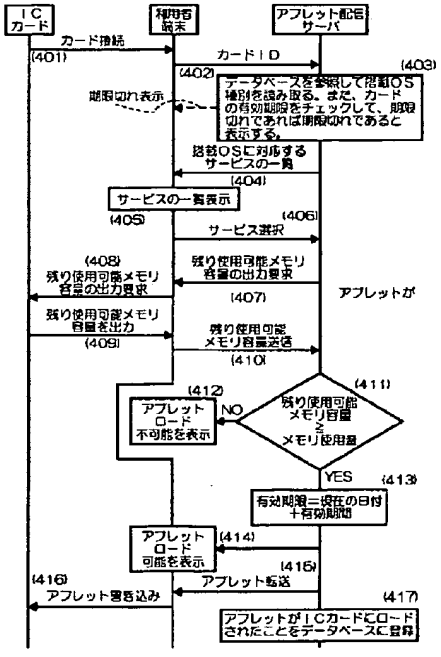
【図２】



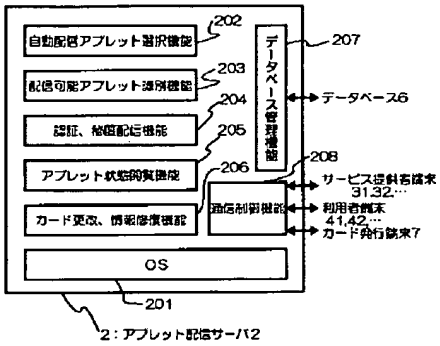
【図７】

カードID	カード種別	OS種別
CDID1	C1	OS1
CDID2	C4	OS1
CDID3	C1	OS2
⋮	⋮	⋮

【図４】



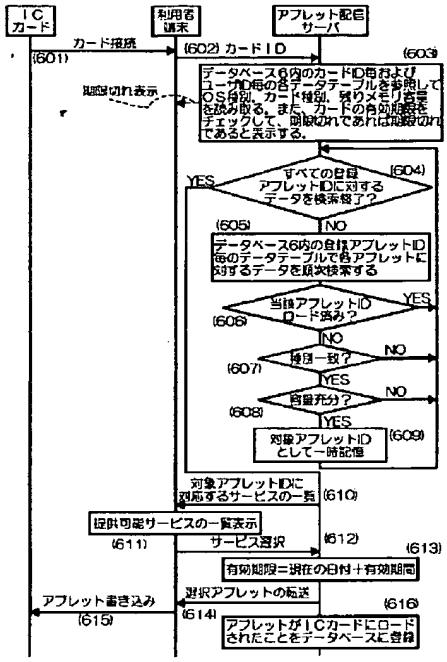
【図３】



【図８】

ユーザID	カードID	アプレットID	ICカード残り使用可能メモリ量	有効期限	カード有効期限
UID1	CDID1	APID1	UM1	P1	Q1
		APID5		P2	
	CDID2	APID6	UM2	P3	Q2
UID2	CDID3	APID2	UM3	P4	Q3
⋮	⋮	⋮	⋮	⋮	⋮

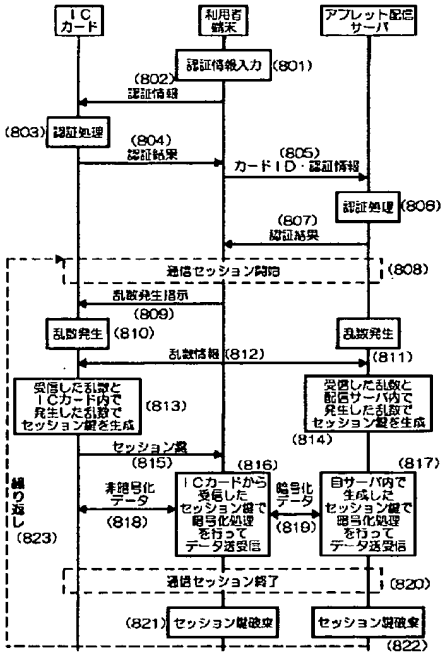
【図５】



【図６】

サービス提供者	サービス名称	OS種別	アプレットＩＤ	対応ＩＣカード種別	メモリ使用量	単位課金情報	ロード回数	有効期間
S1	SV1	OS1	APID1	C1	M1	UC1	N1	R1
		OS2	APID2	C1	M2	UC1	N2	R2
	SV2	OS1	APID3	C2	M3	UC2	N3	R3
		OS2	APID4	C3	M4	UC2	N4	R4
S2	SV3	OS1	APID5	C1,C4	M5	UC3	N5	R5
	SV4	OS1	APID6	C4	M6	UC4	N6	R6
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図９】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ０６Ｋ 19/07		Ｇ０６Ｋ 19/00	Ｊ	５Ｊ１０４
Ｈ０４Ｌ 9/10		Ｈ０４Ｌ 9/00	６２１Ａ	

(72)発明者　鍵山　俊二
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　高橋　史子
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　高橋　真次
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考)　2C005 MA33 MA34 MB10 SA02 SA03 SA06 SA07 SA08 SA12 SA13 SA21 SA25 TA27
5B035 AA06 BB09 CA11
5B058 CA01 KA02 KA06 KA08 KA11 YA20
5B076 BB17 FA00 FB02
5B085 AA08 AC04 AE02 AE12 AE23 AE29
5J104 NA35 NA37 NA40 PA07 PA11